Abstract

The present invention relates to an asymmetrical encryption method. The public key is made up of a large composite number n; the private key is made up of the factors of the composite number. The encryption is made up of a number of iterations of individual encryption steps that are successively reversed during the decryption. In this context, the reversal of an individual encryption step requires the solving of a quadratic equation modulo m **[sic]**. The private key is preferably made up of the large prime numbers p and q. The public key is the product n of these two prime numbers, as well as a comparatively small integer L which is greater than one. The message m is made up of two integral values m_1 and m_2, thus

$$m = (m_1, m_2),$$

both values being in the set $Z_n = \{0,1,2, \ldots ,n-1\}$.

The encryption is accomplished via the equation

$$c=f^L(m) .$$